CRT and Fixed Patterns in Combinatorial Sequences

Muhammad Asad Khan, Amir Ali Khan, and Fauzan Mirza

National University of Sciences and Technology,
Islamabad, Pakistan
{asad.khan, amir.ali, fauzan.mirza}@seecs.edu.pk

Abstract. In this paper, new context of Chinese Remainder Theorem (CRT) based analysis of combinatorial sequence generators has been presented. CRT is exploited to establish fixed patterns in LFSR sequences and underlying cyclic structures of finite fields. New methodology of direct computations of DFT spectral points in higher finite fields from known DFT spectra points of smaller constituent fields is also introduced. Novel approach of CRT based structural analysis of LFSR based combinatorial sequence is given both in time and frequency domain. The proposed approach is demonstrated on some examples of combiner generators and is scalable to general configuration of combiner generators.

Keywords: CRT, LFSR, DFT, combinatorial generators.

1 Introduction

Chinese Remainder Theorem (CRT) is known for centuries as a solution of congruences in number theory and was appeared in a mathematical classics of Sun Tzu, a mathematician in ancinet China. It is termed as one of the jewels of mathematics and has diverse applications in number theory, abstract algebra, theory of automata, digital signal processing and cryptology. Its magical applications have been classified in three 'C's' which are Computing with various aspects of algorithmics and modular computations, Theory of Codes and Cryptography [3]. From an analytical perspective, CRT is basically a manifestation of addressing complex problems through divide and conquer approach. In other words big structures represented mathematically through their smaller parts mapping the harder problems to their smaller equilvalents and making the analysis easy. In the filed of cryptology, CRT has been known for secret sharing schemes, RSA-CRT and rebalanced RSA-CRT. Continual to new contexts of CRT, new results on applications of CRT in analysis of LFSR based sequneces have been presented in this paper.

This paper shows that there exist hidden structures in underlying finite fields related to LFSR based combinatorial sequences which can be exploited through CRT. Number of constituent LFSRs in a combiner generator posses certain fixed patterns in their base finite fields which can be directly mapped through CRT to resultant fields even being combined through non linear functions. These results

are consistent both in time and frequency domain. Direct computation of spectral components in higher fields from smaller field spectral components through CRT is yet a new idea introduced in this paper. CRT based direct relevance of components of smaller fields to higher fields is novel in associated finite fields theory of combinatorial sequence generators and has obvious usefullness in coding theory and cryptology.

The paper is organized as follows: Section 2 describes the mathematical priliminaries on the subject. In section 3, CRT based fixed patterns existing in the product sequences both in time and frequency domain have been deliberated upon. Section 4 covers the generalized case of combinatorial sequence generators and new methodology to compute spectral components in higher fields from spectral components of contituent fields is given. Comparison of computational complexity of proposed methodology of DFT computataions viz-a-viz classical DFT methods is also included in this section. In Section 5, applications of our results on CRT based fixed structures in cryptanalysis are discussed with small example of a combiner generator. The paper is final concluded in Section 6.

2 Mathematical Priliminaries

Classical theory on LFSR sequences and their applications in cryptology can be found in [5], [4] and [12]. In this section, basic fundamentals related to algebraic theory of LFSR sequences and their frequency domain representaions have been presented. By analyzing the sequences in both time and frequency domain simultaneously, fixed structures related to LFSR sequences and underlying finite fields are highlighted which are considered useful in coding theory and cryptanalysis.

Discrete Fourier Transform (DFT) is considered one of the most important discovery in the area of signal processing. DFT presents us with an alternate mathematical tool that allows us to examine the frequency domain behaviour of signals, often revealing important information not apparent in time domain. DFT S_k of an n-point sequence s_i is expressed in terms inner product between the sequence and set of complex discrete frequency exponentials:

$$S_k = \sum_{i=0}^{n-1} s_i e^{-j2\pi ik/n}, \quad k = 0, 1, 2, ..., n-1 \tag{1}$$

The term $e^{-j2\pi ik/n}$ represents discrete set of exponentials. Alternatively, $e^{-j2\pi/n}$ can be viewed as n^{th} root of unity.

Analogous to the classical DFT, a DFT for a periodic signal s_t with period n defined over a finite field $GF(2^m)$ is represented as

$$S_k = \sum_{t=0}^{n-1} s_t \alpha^{tk}, \quad k = 0, 1, 2, ..., n-1 \tag{2}$$

where S_k is k-th frequency component of DFT and α is the primitive element; generator of $GF(2^m)$ with period n [10]. For Inverse DFT, we will have a relation

$$s_t = \sum_{k=0}^{n-1} S_k \alpha^{-tk}, \quad k = 0, 1, 2, ..., n-1 \tag{3}$$

Similarly for polynomials, we have a relation for DFT and IDFT. Having a correspondence between a minimum polynomial and its associated sequence s_t with $s(x) = \sum_{t=0}^{n-1} s_t x^t$ and $S(x) = \sum_{k=0}^{n-1} S_k x^k$, following relation holds for DFT [4]:

$$S_k = s(\alpha^{-k}), \quad k = 0, 1, 2, ..., n-1 \tag{4}$$

and similarly for IDFT:

$$s_t = S(\alpha^t), \quad t = 0, 1, 2, ..., n-1 \tag{5}$$

The same sequence s_t can also be expressed in terms of its trace representation [7]; a linear operator from $GF(2^m)$ to its subfiled $GF(2)$. Let $Tr_1^m(x) = \sum_{k=0}^{m-1} x^{2^k}$ be the trace mapping from $GF(2^m)$ to $GF(2)$, then m sequence s_t can be represented as:

$$s_t = Tr_1^m(\beta\alpha^t) \tag{6}$$

where α is a generator of a cyclic group $GF(2^m)^*$ and is called as primitive element of $GF(2^m)$. Note that $\beta \in GF(2^m)$ and each of its nonzero value corresponds to cyclic shift of the m-sequence generated by an LFSR with primitive polynomial $f(x)$. Importance of this interpretation of m-sequence is that different sequences constructed from root α of primitive polynomial $f(x)$ are cyclic shifts of the same m-sequence. The associated linear space $G(f)$ of dimension m contains 2^m different binary sequences including all 0s sequence as:

$$G(f) = \{\ \tau^i s \mid 0 \ \leq \ i \ \leq \ 2^m - 2 \ \} \bigcup \{0\} \tag{7}$$

where τ is a left shift operator and represents a linear transformation of sequence s_t. According to Blahut's famous theorem, the linear complexity of a peridic sequence over $GF(2^m)$ of period n is equal to the hamming weight of its fourier transform, provided a fourier transform of block length n exists [1]. All DFT components of an LFSR sequence $\in GF(2^m)$.

The zero components in the Fourier spectrum of a sequence over $GF(2^m)$ are related to the roots of a polynomial of that sequence. For example, DFT of an LFSR sequence with feedback polynomial $f(x) = x^3+x+1$ initialized with state 001 is $0, 0, 0, \alpha^4, 0, \alpha^2, \alpha$. As roots of $f(x)$ are α alongwith its conjugates i.e. α^2 and α^4, so first, second and fourth spectral components are zero. Indices of non zero DFT points for LFSR with minimum polynomial and no multiple roots also follow a fixed pattern. If k-th component of spectral sequence is non zero then all $(2^j k)\ mod\ n$ components will be harmonics of the k-th component where $1 \leq j \leq m-1$. As DFT of a time domain signal comprises of a fundamental frequency and its harmonics, DFT of an LFSR sequence based on a minimal polynomial with

no multiple roots also comprises of $\alpha^i \in GF(2^m)$ and its harmonics $\alpha^{i^j \, mod \, n} \in GF(2^m)$ with $0 \leq i \leq n-1$. This harmonic pattern can be efficiently exploited in cryptanalysis attacks on LFSR based sequence generators.

Let two sequences related by a time shift $u_t = s_{t+\tau}$, their DFTs U_k and S_k are related as:

$$U_k = \alpha^{k\tau} S_k, \qquad k = 0, 1, ..., n-1 \tag{8}$$

Indices of non-zero spectral points of an LFSR sequence does not change with the shift in LFSR sequence. A non-zero k-th component of DFT of an LFSR sequence will always be non-zero. Any shift in LFSR sequence will only change the value at this component by Equation (8). Converse is also true for zero spectral points of an LFSR sequence which will always be zero no matter how much sequence is shifted.

A binary sequence s_t can be represented in terms of trace function with spectral componenets as follows:-

$$s_t = \sum_{j \in \Gamma(n)} Tr_1^{m_j}(A_j \alpha^{-jt}), \qquad t = 0, 1, ..., n-1 \tag{9}$$

where $Tr_1^{m_j}$ is a trace function from $GF(2^m)$ to $GF(2)$, $A_j \in GF(2^m)$ and $\Gamma(n)$ is a set of cyclotomic coset leaders modulo n.

3 CRT and Underlying Finite Field Theory of Product Sequences

In this section, analysis of a product sequence generated through multiplication of two LFSRs sequences is presented which includes new results on underlying algebraic theory of finite fields. A CRT based linear structure existing in the time and frequency domain representation of the product sequence is presented which renders itself useful for coding theory and cryptanalysis of LFSR based sequence generators. We build our analysis by starting with a simple case of multiplication of output sequences of two LFSRs and illustrate our novel observations on fixed structures existing in the time as well as frequency domian representation of product sequences. The observations of this special case will be generalized to a combinatorial generators in the next section.

Theorem 1. *Let $s_t \in GF(2^m)$ be a reference product sequence with period $n \mid 2^m - 1$ having two constituent LFSRs defined over primitive polynomials with individual periods n_1 and n_2. With different shifts k_1 and k_2 in initials states of LFSRs, resulting output sequnece u_t is correlated to s_t by $u_t = s_{t+\tau}$ where shift τ is determined through CRT as*

$$\begin{aligned} \tau &\equiv k_1 \pmod{n_1} \\ \tau &\equiv k_2 \pmod{n_2} \end{aligned}$$

Proof. Within a cyclic group $GF(2^m)$, associated linear space $G(f)$ of dimension m contains $2^m - 1$ non-zero binary sequences by (7).
As s_t and u_t both $\in GF(2^m)$, they are shift equilvalents by (**??**) with unknown shift value of τ.
The product sequnec s_t of a_t and b_t can be expressed as

$$s_i = a_j.b_v \tag{10}$$

where $0 \le i \le n-1$, $0 \le j \le n_1 - 1$ and $0 \le v \le n_2 - 1$.

Axiom 1. *While contributing towards a product sequence of length n with two LFSRs, stream of LFSR-1 defined over $GF(2^p)$ with primitive polynomial and its maximum period $2^p - 1$ is repeated δ_1 times while LFSR-2 defined over $GF(2^q)$ with primitive polynomial as well and corresponding period $2^q - 1$ is repeated δ_2 where*

$$\delta_1 = \frac{lcm(n_1, n_2)}{n_1}\ , \quad and$$
$$\delta_2 = \frac{lcm(n_1, n_2)}{n_2}$$

Axiom 2. *Within a sequence of period n for a product sequence, each value of index j corresponds to all values of index v if and only if $gcd(n_1, n_2) = 1$.*

From Axioms 1 and 2, any shift in LFSRs initial states will produce output corresponding to some fixed indices of j and v which already existed in the refernce sequence at some fixed place with initial states of LFSRs without shift.

With known values of j and v i.e. $k_{i's}$, CRT will give us the value of τ mod n as

$$\tau \equiv k_1 \pmod{n_1}$$
$$\tau \equiv k_2 \pmod{n_2}$$

□

Let we explain the facts with an example.

Example 1. Let we have a sequence s_t generated from product of two LFSRs having primitive p[olynomials of $g_1(x) = x^2 + x + 1$ and $g_2(x) = x^3 + x + 1$. The period n_1 of stream a_t corresponding to LFSR-1 is 3 and n_2 of b_t corresponding to LFSR-2 is 7. The period n of s_t is 21.

Table 1 demonstrates product of two m sequences generated from these two LFSRs.

Table 1. Product sequence of 2x LFSRs with $n_1 = 3$ and $n_2 = 7$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_1	b_2	b_3	b_4	b_5	b_6	b_7
s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}	s_{17}	s_{18}	s_{19}	s_{20}	s_{21}

We analyze the impact of shift on LFSR sequences and their behaviour in cyclic stuctures of finite fields involved. We will shift the LFSR sequences one by one and observe the fixed patterns which can be exploited in cryptanalysis of the combiner generators in particular. We can represent shifts in LFSRs sequences with k and l as

$$s_t = a_{i+k}.b_{i+l}\ , \qquad \text{with } 0 \leq\ i\ \leq n-1 \tag{11}$$

where $k \in [0, n_1 - 1]$ and $l \in [0, n_2 - 1]$. Table 2 demonstrates the scenerio where a_t is left shifted by one bit while keeping the b_t fixed with initial state of '1'.

Table 2. Product sequence with a_t shifted left

7	8	9	10	11	12	13	14	15	16	17	18	19	20	0	1	2	3	4	5	6
a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_1	b_2	b_3	b_4	b_5	b_6	b_7
s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}	s_{17}	s_{18}	s_{19}	s_{20}	s_{21}	s_1	s_2	s_3	s_4	s_5	s_6	s_7

Comparison of Table 1 with Table 2 reveals that shifting one bit left of a_t and fixing the b_t to reference initial state of '1' shifts s_t by seven units left. Similarly, shifting another bit of a_t to left, brings a_3 corresponding to b_1 which can be located in Table 1 at shift position 14. So two left shifts of a_t shifts s_t by 14 units left with reference to bit positions in Table 1. Now we analyze the impact of left shift of b_t on s_t. Table 3 demonstrates the scenerio where b_t is left shifted by one bit while keeping the a_t fixed with initial state of '1'.

Table 3. Product sequence with b_t shifted left

15	16	17	18	19	20	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3	a_1	a_2	a_3
b_2	b_3	b_4	b_5	b_6	b_7	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_1
s_{16}	s_{17}	s_{18}	s_{19}	s_{20}	s_{21}	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}

It can be easily seen that one left shift in b_t shifts s_t by 15 units where b_2 is corresponding to a_1. Similarly, another left shift in b_t shifts s_t by another 15 units bringing the b_3 corresponding to a_1. Subsequently, three left shifts in b_t with reference to initial state of '1' brings b_4 corresponding to a_1 which is at shift index-3 in Table 1. Similar fixed patterns can be observed for simultaneous shifts of LFSRs and it will be discussed with more detail in following paragraphs.

Let us model this fixed patterns in LFSRs cyclic structures and shifts in intial states of LFSRs through CRT as

$$
\begin{aligned}
x &\equiv k \pmod{n_1} \\
x &\equiv l \pmod{n_2}
\end{aligned}
$$

where k and l denote the amount of shifts in initial state of individual LFSRs with reference to initial state of '1'. The solution of CRT i.e. $x(\bmod\ r)$ gives the amount of shift in s_t with reference to u_t as depicted in (**??**). Consider a scenerio again where a_t is shifted left by one bit and b_t is fixed with initial state of '1' and can be expressed as

$$
\begin{aligned}
x &\equiv 1 \pmod{3} \\
x &\equiv 0 \pmod{7}
\end{aligned}
$$

The CRT gives the solution of 7(mod 21) which is index position of a_2 corresponding to b_1 in Table 1 shifting the product sequence s_t by seven units left. Consider another scenerio of simultaneous shifts in both LFSRs sequences where a_t is shifted left by one bit and b_t is shifted left by 3 bits with reference to their initial states of '1' and can be expressed as

$$
\begin{aligned}
x &\equiv 1 \pmod{3} \\
x &\equiv 3 \pmod{7}
\end{aligned}
$$

The CRT gives value of -11 which is 10 (mod 21), representing the product sequence u_t as 10 units left shifted version of s_t. This value matches to index position of b_4 corersponding to a_2 in Table 1.

Our Observations related to direct correspondence of shift index with initial states of LFSRs and CRT calculations done modulo periods of individual LFSRs are valid for any number of LFSRs in different configurations of nonlinear sequence generators. These observations on classical theory of LFSR cyclic structures with their CRT based interpretation are considered significant for cryptanalysis.

In addition to the results of Blahut's theorem on time and frequency domain relationship of sequences, an important corollary establishes new facts related fourier transform in binary fields.

Corollary 1. *Let $s_t \in GF(2^m)$ be a product sequence with period $n \mid 2^m - 1$ having two constituent sequences $a_t \in GF(2^p)$ and $b_t \in GF(2^q)$ of LFSRs each*

defined over primitive polynomials with individual periods $n_1 = 2^p - 1$ and $n_2 = 2^q - 1$. If A be a DFT spectra of a_t, B be a DFT spectra of b_t and S be a DFT spectra of s_t, non zero spectral components of S will only exist at those indices where spectral components of A and B are non zero.

we have another associated corollary here:-

Corollary 2. *With known non zero spectral components of A and B, non zero spectral components of S can be directly determined through Chinese Remainder Theorem (CRT) as:*

$$x \equiv k_1 \quad (mod\, n_1)$$
$$x \equiv k_2 \quad (mod\, n_2)$$

where k_1 and k_2 are non zero index positions of A_k and B_k respectively and x is the position of non zero componenet of DFT spectra of s_t within its period n.

It is important to observe here that indices of non zero spectral components present in a complete spectrum of resultant stream are determined while working in base fields of component LFSRs and without computing DFT of s_t in a larger field. Let we explain these corollaries through a small example here.

Example 2. Following the Example 1, consider a product sequence s_t generated from two LFSRs with minimum polynomials $g_1(x) = x^3 + x + 1$ and $g_2(x) = x^2 + x + 1$.

1. In time domain representation, we have following sequences.
   Sequence a_t: 011 (of period 3)
   Sequence b_t: 0010111 (of period 7)
   Sequence s_t: 001011000001010010011101110111011101 (of period 21)
2. From (2), frequency domain representations of these sequences are:
   (a) $A = 0, 1, 1$
   (b) $B = 0, 0, 0, \alpha^4, 0, \alpha^2, \alpha$
   (c) To compute S, associated minimum polynomial is determined through Berlekamp-Massey algorithm which is $g(x) = x^6 + x^4 + x^2 + x + 1$.
   $S = 0, 0, 0, 0, 0, \alpha^9, 0, 0, 0, 0, \alpha^{18}, 0, 0, \alpha^{15}, 0, 0, 0, \alpha^{18}, 0, \alpha^9, \alpha^{15}$

Non-zero DFT points in S clearly follow a linear behaviour as of time domain representation where any k-th component is non-zero if and only if A_k and B_k are both non-zero. Through non zero indices of A and B, CRT can be directly used to determine non-zero spectral points of S. For instance,

$$x \equiv 1 \pmod 3$$
$$x \equiv 3 \pmod 7$$

results into index 10 where α^{18} is a non zero spectral component of S. These results on determining non zero spectral indices for product of two sequences are valid for product sequences containing more number of LFSRs as well.

Harmonic pattern of DFT spectra are visible for A, B and S. Non-zero indices of DFT sequences also follow a fixed pattern. In case of S, non zero DFT element at index 5 has its harmonics at indices 10, 20, 19 (40 mod 21), 17 (80 mod 21) and at 13 (160 mod 21). The zero components in the fourier transform of a product sequence s_t defined over $GF(2^m)$ are related to roots of $g_(x) = x^6 + x^4 + x^2 + x + 1$. As roots of $g(x)$ are α alongwith its conjugates i.e. α^2, α^4, α^8 and α^{16} so first, second, fourth, eigth and sixteenth spectral components are zero.

4 Computing the Spectral Components in $GF(2^m)$ through CRT

Computing DFT of a sequence $\mathbf{s} \in GF(2^m)$ by equation (2) over binary fields requires determining the associated minimum polynomial $m(x)$ of s. The most efficient method which computes the linear complexity l of a periodic sequence s and gives its minimum polynomial is berlekamp massey algorithm [4]. The algorithm further requires $2l$ bits of the sequence to determine the linear complexity and minimum polynomial $m(x)$. Based on the root of minimum polynomial $m(x)$, equation 2 requires complete period of the sequence to compute each spectral componenet of S. Faster method to compute DFT in binary fields proposed in [8] requires lesser number of bits equal to linear complexity l or in few cases lesser than that. However, in all these cases computations have to be in $GF(2^m)$ to which sequence s belongs. In this section, new method has been introduced which allows mapping of spectral components of smaller constituent fields to larger finite fields with few limitations of choice of particular indices. We will develop our idea progressively from product of sequences in time domain to a genarlized case of boolean functions where addition of bits in $GF(2)$ is encompassed as well.

4.1 Product of Arbitrary Number of m-Sequences

In this subsection, case of product sequence is considered where any arbitrary number of LFSR sequences are multiplied togather. Starting with simple case of two LFSRs, we will establish facts for more number of LFSRs where direct computation of spectral points for product sequence is done from DFT points of individual LFSR sequences. We have an important theorem here.

Theorem 2. *Let $s_t \in GF(2^m)$ be a product sequence with period $n \mid 2^m - 1$ having r constituent sequences $a_i \in GF(2^{p_i})$ of LFSRs each defined over primitive polynomials with individual periods $n_i = (2^{p_i} - 1)$, where all n_i are coprime to each other and $0 \leq i \leq r-1$. Let A^i be a DFT spectra of a_i, a k-th spectral component of S corresponding to each non-zero spectral components of $A^i_{(k \ mod \ n_i)}$ can be determined directly through CRT as*

$$
\begin{aligned}
d &\equiv d_1 \quad (mod\, n_1)\\
d &\equiv d_2 \quad (mod\, n_2)\\
&.. \;..\; ....\\
&.. \;..\; ....\\
d &\equiv d_r \quad (mod\, n_r)
\end{aligned}
$$

where d, d_1, d_2,..., d_r are degrees of non-zero spectral components i.e. S_k, $A^1_{(k\ mod\ n_1)}$,..., $A^r_{(k\ mod\ n_r)}$ respresented in terms of associated roots $\gamma \in GF(2^m)$, $\alpha_1 \in GF(2^{p_1})$, $\alpha_2 \in GF(2^{p_2})$, ... and $\alpha_r \in GF(2^{p_r})$ of minimal polynomials of $\boldsymbol{s}$, $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ... and $\boldsymbol{a}_r$ respectively.

Proof. To prove the theorem for a generalized case of r LFSRs multiplied togather, let we consider first a simple case of product of two LFSRs only.

Let $s_t \in GF(2^m)$ be a product sequence with period $n \mid 2^m - 1$ having two constituent sequences $a_t \in GF(2^p)$ and $b_t \in GF(2^q)$ of LFSRs each defined over primitive polynomials with individual periods $n_1 = (2^p - 1)$ and $n_2 = (2^q - 1)$, where n_1 and n_2 are coprime to each other. Let A be a DFT spectra of a_t, B be a DFT spectra of b_t and S be a DFT spectra of s_t.

Let d, d_1 and d_2 are degrees of non-zero spectral components i.e. S_k, $A_{(k\ mod\ n_1)}$ and $B_{(k\ mod\ n_2)}$ respresented in terms of associated roots $\gamma \in GF(2^m)$, $\alpha \in GF(2^p)$ and $\beta \in GF(2^q)$ of minimal polynomials of s_t, a_t and b_t respectively. All roots of minimum polynomials of a, b and s lie within their respective fields i.e. $\alpha \in GF(2^p)$, $\beta \in GF(2^q)$ and $\gamma \in GF(2^m)$ respectively. n_1 and n_2 being coprime, $n = lcm(n_1, n_2)$. By corollary 2, spectral components of S are non zero at all indices where corresponding spectral components of A and B are non zero. As all DFT spectral components of S lie within $GF(2^m)$ and correspond to γ^h, where $0 \leq h \leq m-1$. Let we consider any k-th component of spectra of S corresponding to non zero DFT components of A and B, where we only need to prove that both non zero spectral components of A and B has one to one mapping to S through CRT.
Transforming the relationship of s_t= $a_t.b_t$ into roots of associated polynomials of each sequence in their respective binary fields by using definitions of $GF(2^m)$ by γ^h $(0 \leq h \leq n)$, $GF(2^p)$ by α^i $(0 \leq i \leq n_1)$ and $GF(2^q)$ by β^j $(0 \leq j \leq n_2)$, we have

$$\gamma^d = \alpha^d.\beta^d, \quad d = 0, 1, 2, ..., n-1 \tag{12}$$

As we can write s_t= $a_{(t\ mod\ n_1)}.b_{(t\ mod\ n_2)}$, equation (12) can be expressed as

$$\gamma^d = \alpha^{d\ mod\ n_1}.\ \beta^{d\ mod\ n_2}, \quad t = 0, 1, 2, ..., n-1 \tag{13}$$

From equation (13), there exists a unique mapping for γ^d, α^{d_1}, and β^{d_2} which can be computed using CRT as

$$
\begin{aligned}
d &\equiv d_1 \pmod{n_1}\\
d &\equiv d_2 \pmod{n_2}
\end{aligned}
$$

Mapping these facts on a product sequence having r constituent sequences, it becomes trivial to see

$$\begin{aligned} d &\equiv d_1 \pmod{n_1} \\ d &\equiv d_2 \pmod{n_2} \\ &.. \; .. \; .... \\ &.. \; .. \; .... \\ d &\equiv d_r \pmod{n_r} \end{aligned}$$

□

As $GF(2^m)$ considered here is implicitly constituted by product of elements of $GF(2^p)$ and $GF(2^q)$, convolution of $\alpha^i \in GF(2^p)$, $\beta^j \in GF(2^q)$ should result into spectral component $\gamma^h \in GF(2^m)$ ideally at each index k . For convolutions in finite fields, readers may refer to [11]. However, when elements belong to different binary fields, not much is known to us . Nevertheless, CRT based method of computing DFT components in higher binary fields from constituent DFT components in lower order fields is considered novel in this regard. Let us illustrate our results through an example.

Example 3. Consider a product sequence $\mathbf{s}$ having three LFSRs with primitive polynomials as $g_1(x) = x^2 + x + 1,\ g_2(x) = x^3 + x + 1$ and $g_3(x) = x^5 + x^2 + 1$. The outputs of LFSRs in this case are m-sequences, denoted as $\mathbf{a}^1$, $\mathbf{a}^2$ and $\mathbf{a}^3$ respectively. Product stream $\mathbf{s}$ is obtained as

$$s_t = a_t^1.a_t^2.a_t^3 \quad \text{where } 0 \leq t \leq n-1 \tag{14}$$

where period n of $\mathbf{s}_t$ in this case becomes 651 as $\mathrm{lcm}(3, 7, 31) = 651$. DFT components of $\mathbf{a}$, $\mathbf{b}$, and $\mathbf{c}$ with primitive elements $\alpha \in GF(2^2)$, $\beta \in GF(2^3)$ and $\delta \in GF(2^5)$ respectively are

- $\mathbf{A}^1 = \{0, 1, 1\}$
- $\mathbf{A}^2 = \{0, 0, 0, \beta^4, 0, \beta^2, \beta\}$
- $\mathbf{A}^3 = \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \delta^{29}, 0, 0, 0, 0, 0, 0, 0, \delta^{30}, 0, 0, 0, \delta^{15}, 0, \delta^{23}, \delta^{27}\}$

To compute DFT of $\mathbf{s}$, we need to compute its associated minimum polynomial through berlekamp massey algorithm which in this case is $m(x)$= $x^{30} + x^{25} + x^{24} + x^{20} + x^{19} + x^{17} + x^{16} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^4 + x^2 + 1$ with generator $\gamma \in GF(2^{30})$.
Having a complete period (651 bits) of $\mathbf{s}$, we compute DFT through equation 2. Corresponding to degree of minimum polynomial, we get thirty non-zero DFT components at indices shown in Table 4 below.

Table 4. Non Zero Spectral Points of **S**

Index	61	89	122	139	178	185	209	215	244	271
Spectral Component	γ^{492}	γ^{387}	γ^{333}	γ^{246}	γ^{123}	γ^{585}	γ^{309}	γ^{240}	γ^{15}	γ^{30}
Index	278	325	356	370	395	418	430	433	461	488
Spectral Component	γ^{492}	γ^{60}	γ^{246}	γ^{519}	γ^{123}	γ^{618}	γ^{480}	γ^{120}	γ^{15}	γ^{30}
Index	523	542	556	587	619	635	643	647	649	650
Spectral Component	γ^{387}	γ^{60}	γ^{333}	γ^{519}	γ^{585}	γ^{618}	γ^{309}	γ^{480}	γ^{240}	γ^{120}

From corollary 2, non zero indices of **S** can be determined directly from knowing the individual DFTs of three LFSRs separately. For instance,

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 15 \pmod{31} \end{aligned}$$

gives result of 325 which exists amongst thirty non-zero DFT computations as well. Similarly with known spectral points of $\mathbf{A}_1^1 = \alpha^0$, $\mathbf{A}_3^2 = \beta^4$ and $\mathbf{A}_{15}^3 = \delta^{29}$, spectral component $\mathbf{S}_{325}$ can be determined directly by theorem 2 as

$$\begin{aligned} d &\equiv 0 \pmod 3 \\ d &\equiv 4 \pmod 7 \\ d &\equiv 29 \pmod{31} \end{aligned}$$

CRT gives the result of 60. So the spectral componenet $\mathbf{S}_{325} \in GF(2^{30})$ becomes γ^{60}. Similarly all non zero points of $\mathbf{S} \in GF(2^{30})$ can be computed directly by theorem 2 without the requirement of minimum polynomial $m(x)$, n number of bits of **s** and classical computations of DFT by equation 2. Conversely, from known DFT spectra of **S** only, individual DFT spectral points of $\mathbf{A}^1$, $\mathbf{A}^2$ and $\mathbf{A}^3$ can also be computed. For instance, having known γ^{492} at S_{61}, $\mathbf{A}_1^1$ is directly computed as α^0, $\mathbf{A}_5^2$ is computed as β^2 and $\mathbf{A}_{30}^3$ is computed as δ^{27}. These results are considered very useful in cryptanalysis of LFSR based sequences.

4.2 Generic Combinatorial Sequences

Having considered the product sequences of multiple LFSRs, generic case of combinatorial sequences is discussed now where outputs of multiple LFSRs are combined through a non linear function involving multiplication and addition of bits in $GF(2)$. From the established fact of theorem 2 for product sequenecs, we now generalize the case for combinatorial generators here.

Consider a combinatorial generator consisting of r constituent LFSRs. Let $z_t \in GF(2^m)$ be the output sequence of generator with period $n \mid 2^m - 1$ and

$m(x)$ be the associated minimum polynomial. Let $\gamma \in GF(2^m)$ be the root of $m(x)$, $\alpha_1 \in GF(2^{p_1})$, $\alpha_2 \in GF(2^{p_2})$, ... and $\alpha_r \in GF(2^{p_r})$ of minimal polynomials of $\mathbf{z}$, $\mathbf{a}_1$, $\mathbf{a}_2$, ... and $\mathbf{a}_r$ respectively. The nonlinear function $f(x_1, x_2, ..., x_{r-1})$ combines outputs of $\mathbf{r}$ LFSRs and produces the resultant stream $\mathbf{z}$ as

$$z_t = f(a_t^1, a_t^2, ...a_t^r) \quad \text{where } \ 0 \leq t \leq n-1 \tag{15}$$

As $f(x)$ is not only a product function, we have

$$m(x) \neq m_1(x).m_2(x)....m_r(x) \tag{16}$$

$$\Rightarrow \gamma \neq \alpha^1.\alpha^2....\alpha^r \tag{17}$$

To take DFT of $\mathbf{z}$ by Equation 2, we require n bits of $\mathbf{z}$ and DFT will be computed with respect to $\gamma \in GF(2^m)$ having order n. Non zero DFT terms termed as linear span of $\mathbf{z}$ will be equilavalent to degree of associated minimum polynomial $m(x)$. These results are consistent to known theory of DFT in binary fields. However, few additional results are noted which are correlated to CRT based fixed patterns of sequences.

If we take DFT of $\mathbf{z}$ with respect to generator σ of its minimum polynomial $m(x)$, experimental results reveal that irrespective of combining function $f(x)$, a fixed relationship between frequency components of $\mathbf{Z}$ and individual spectral components of $\mathbf{A}^1$,$\mathbf{A}^2$,....,$\mathbf{A}^r$ exists at all those indices of $\mathbf{Z}$ where corresponding spectral components of $\mathbf{A}^1$,$\mathbf{A}^2$,....,$\mathbf{A}^r$ are all non zero. Let we represent d, d_1, d_2,..., d_r as degrees of non-zero spectral components of Z_k, $A^1_{(k \ mod \ n_1)}$,..., $A^r_{(k \ mod \ n_r)}$ respresented in terms of associated roots of respective minimum polynomials. At any index k, where all corresponding spectral components of LFSR sequenecs are non zero, $\mathbf{Z}_k \in GF(2^m)$ can be directly determined using through CRT as described in theorem 2. Similarly, from corollary 2 and **??**, non zero indices of $\mathbf{S}$ corresponding to non zero spectral components of $\mathbf{A}^1$,$\mathbf{A}^2$,....,$\mathbf{A}^r$ are directly determined. Let we validate our observations through an example of a simple combiner generator.

Example 4. With the same assumptions of Example 3 with three LFSRs and notations used therein, output stream $\mathbf{z}_t$ of a combiner is obtained as

$$z_t = a_t^1.a_t^2 + a_t^2.a_t^3 + a_t^3.a_t^1 \quad \text{where } \ 0 \leq t \leq n-1 \tag{18}$$

Taking the DFT of $\mathbf{z}$ by Equation 2 with respect to $\gamma \in GF(2^{30})$ as a generator of $(x^{30}+x^{25}+x^{24}+x^{20}+x^{19}+x^{17}+x^{16}+x^{13}+x^{10}+x^9+x^8+x^7+x^4+x^2+1)$ with generator $\gamma \in GF(2^{30})$, 31 non zero DFT points are mentioned in Table 5 below.

Table 5. Non Zero Spectral Points of $\mathbf{Z}$

Index	27	31	54	62	77	91	108	124	153	156
Spectral Component	γ^{15}	γ^{186}	γ^{30}	γ^{372}	γ^{123}	γ^{60}	γ^{309}	γ^{93}	γ^{519}	γ^{30}
Index	182	201	213	216	248	306	308	339	341	364
Spectral Component	γ^{492}	γ^{618}	γ^{480}	γ^{120}	γ^{186}	γ^{618}	γ^{387}	γ^{333}	γ^{93}	γ^{30}
Index	371	402	426	432	495	496	511	573	581	612
Spectral Component	γ^{387}	γ^{585}	γ^{309}	γ^{240}	γ^{492}	γ^{372}	γ^{309}	γ^{246}	γ^{240}	γ^{123}
Index	616									
Spectral Component	γ^{387}									

Linear complexity of z_t is determined to be 31 through berlekamp-massey algorithm and the corresponding minimum polynomial $m(x)$ in this case is: $(x^{31} + x^{29} + x^{28} + x^{27} + x^{24} + x^{23} + x^{22} + x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1)$. Now DFT is taken with respect to generator $\sigma \in GF(2^{31})$ of $m(x)$ with order 651. We will only mention spectral points at those indices where constituent LFSR sequences have all non zero spectral points.

Table 6. Non Zero Spectral Points of $\mathbf{Z}$ with element σ of $m(x)$

Index	61	89	122	139	178	185	209	215	244	271
Spectral Component	σ^{492}	σ^{387}	σ^{333}	σ^{246}	σ^{123}	σ^{585}	σ^{309}	σ^{240}	σ^{15}	σ^{30}
Index	278	325	356	370	395	418	430	433	461	488
Spectral Component	σ^{492}	σ^{60}	σ^{246}	σ^{519}	σ^{123}	σ^{618}	σ^{480}	σ^{120}	σ^{15}	σ^{30}
Index	523	542	556	587	619	635	643	647	649	650
Spectral Component	σ^{387}	σ^{60}	σ^{333}	σ^{519}	σ^{585}	σ^{618}	σ^{309}	σ^{480}	σ^{240}	σ^{120}

Now we apply our observations on CRT based fixed patterns in sequences and compute spectral components of $\mathbf{Z}$ directly by using Theorem 2. From individual DFTs of LFSR sequences as computed in Example 2, corresponding to non zero indices of $\mathbf{A}^1$, $\mathbf{A}^2$ and $\mathbf{A}^3$, we first determine non zero index of $\mathbf{Z}$ through CRT using Equation 2 as

$$
\begin{aligned}
x &\equiv 2 \pmod 3 \\
x &\equiv 6 \pmod 7 \\
x &\equiv 30 \pmod{31}
\end{aligned}
$$

we get index of 650. Now we compute spectral value of $\mathbf{Z}_{650}$ respresented in terms of $\sigma \in GF(2^{31})$ through CRT using Theorem 2 as

$$d \equiv 0 \pmod 3$$
$$d \equiv 1 \pmod 7$$
$$d \equiv 27 \pmod{31}$$

we get $\mathbf{Z}_{650}=\sigma^{120}$. Spectral components of other non zero indices of $\mathbf{Z}$ along with all values of σ^i with order 651 are mentioned at appendix A. These results reveal that irrespective of non linear function $f(x)$, degree of spectral components corresponding to spectra of constitunet LFSR sequences is consistent even being in different fields. For instance $\mathbf{Z}_{650}=\sigma^{120}$ for a generalized combiner case and $\mathbf{S}_{650}=\gamma^{120}$ for a product case (Example 2) have same degree with different values of spectral components being $\sigma \in GF(2^{31})$ and $\gamma \in GF(2^{30})$.

4.3 Complexity of CRT Based DFT Computations

In this subsection, discussion on computational complexity of CRT based DFT calculations in comparison to classical DFT is presented. DFT in binary fields from Equation 5 dictates that the complexity for computing each $\mathbf{S}_k$ is equilvalent to cost for evaluating polynomial $s(x)$ at α^{-k} [6] where $\psi = \alpha^{-k}$. In terms of exclusive-or operations, we have:-

1. The complexity of computing minimum polynomial of a sequence $\in GF(2)$ through berlekamp massey algorithm is $\mathcal{O}(m\ log\ m)$.
2. The complexity of multiplying two polynomials of degree m is
$$\mathcal{O}(m\ log\ m\ log\ log\ m)$$
3. The complexity of solving system of r linear equations over $GF(2^m)$ is
$$\mathcal{O}(r^{2.37}\ m\ log\ m\ log\ log\ m)$$
4. The complexity in terms of Xor operations for computing each $\mathbf{S}_k$ using the Equation 5 is
$$\mathcal{O}((\ m\ log\ m\ log\ log\ m)[(log\ (k) + deg(s(x))])$$

For CRT based computations of spectral components from constituent spectral components, we will consider a case of product of two LFSR sequences which can be generalized for a combiner generator. Let we have two sequences $\mathbf{a} \in GF(2^p)$ and $\mathbf{b} \in GF(2^q)$. It is trivial to mention that

$$\text{Complexity of DFT } (\mathbf{s}) \gg \text{Complexity of [DFT } (\mathbf{a}) + \text{DFT } (\mathbf{b})]$$

For each $\mathbf{S}_k$, additional computational complexity for CRT is $\mathcal{O}(len(n)^2)$. As non zero terms of $\mathbf{S}_k$ are equilavalent to the linear span of the sequence, thus total cost of CRT based computataional step of spectral components is $\mathcal{O}(LS(s)\ .\ len(n)^2)$, where LS is linear span of the sequence $\mathbf{s}$. Thus CRT based computations of spectral components of $\mathbf{s}$ for combiner generators are far efficient than classical methods of DFT computations in binary fields.

5 CRT and Cryptanalysis of Combiner Generators

In this subsection, discussion on application of our novel results on CRT based fixed patterns in cryptanalysis of combiner sequences is made. From discussion made in Section 3 on established linkage between period of LFSR sequence, effect of left shifts of LFSR initial states and mathe- matical rationale through CRT, let we demonstrate application of our observations on analysis of combiner generators.

Example 5. With same structure of combiner generator mentioned in Example 4, suppose we know 10 bits of keystream u_t = [1011110001]. During off-line computations, we will generate 651 bits of reference stream i.e. s_t with initial fills of all three LFSRs as '1' which comes out to be:
00101101011101101101101101101010101101101100101110001101101101
1100101110110111101001100101110100101001011 10................... 1010
11010010111001011110001111010111

Comparing the ten known bits of keystream u_t = [1011110001] with reference sequence s_t , index position of known bits is determined as k=632. Thus

$$u_i = s_{i+632}, \qquad \forall\ i\ \geq 0.$$

After determining index position of ten known bits of u_t in reference stream s_t, we will determine initial states of LFSR by simply applying modular computations of CRT as follows:

$$\begin{aligned} k_1 &\equiv 632 \pmod{3} \\ k_2 &\equiv 632 \pmod{7} \\ k_3 &\equiv 632 \pmod{31} \end{aligned}$$

Therefore, $k_1 \equiv 2 \pmod 3$, $k_2 \equiv 2 \pmod 7$ and $k_3 \equiv 12 \pmod{31}$. By using Equation 6, initial states of LFSRs is determined as given in Table 7 below.

Remark 1. Generating the complete period of reference sequence $\mathbf{s}_t$ followed by finding few known bits of available keystream $\mathbf{u}_t$ in a complete period of $\mathbf{s}_t$ may not be computationally feasible for sequence of larger periods which infact is the case of practical stream ciphers. However, the example is given to demonstrate the existing cyclic structures of LFSR based sequences designs and their CRT based interpretation.

Now, let frequency domain analysis of combiner sequences is made in the light of our results on CRT based relevance of spectral components. With the same notataions as of Example 4, if spectral component $\mathbf{Z}_k$ is computed from known ciphertext stream by any method where k corresponds to all non zero unknown spectral componenets of constituent LFSR sequences, these individual spectral componenets are computed using Theorem 2 and Corollary 2. With

known spectral components of constituent LFSRs, initial states of LFSRs is determined by using Equation (8) and (6). For instance, for $\mathbf{Z}_{650}$=σ^{101}, we will do modular computations to determine the spectral component of individual LFSRs as

$$101 \equiv 2 \pmod 3$$
$$101 \equiv 3 \pmod 7$$
$$101 \equiv 10 \pmod{31}$$

We get $\alpha^2 \in GF(2^2)$ at $\mathbf{A}_2^1$, $\beta^3 \in GF(2^3)$ at $\mathbf{A}_6^2$ and $\gamma^{10} \in GF(2^5)$ at $\mathbf{A}_{30}^3$. Now shift value for each LFSR is computed using Equation (8) as

$$\alpha^\tau = (Z_k.S_k^{-1})^{k^{-1}} \qquad (19)$$

where τ determines the exact amount of shift between s_t and z_t and k is index of any one component of DFT spectra.

Having determined the exact shift value for each LFSR, their initial states will be computed using Equation (6) within each subfield $GF(2^j)$ as

$$b_t^1 = Tr_1^n(\alpha^* \alpha^t)$$
$$b_t^2 = Tr_1^n(\beta^* \beta^t)$$
$$b_t^3 = Tr_1^n(\gamma^* \gamma^t)$$

where

$$\alpha_i^* = \alpha^{\tau_i}$$
$$\beta_j^* = \beta^{\tau_j}$$
$$\gamma_l^* = \gamma^{\tau_l}$$

The initial fills of LFSRs with refernce to intial state of '1' for all LFSRs with 1 left shift in a_t^1, 5 left shifts in a_t^2 and 19 left shifts in a_t^3 gives:

Table 7. Initial States of 3 LFSRs

	Initial State
LFSR-1	10
LFSR-2	101
LFSR-3	01111

Remark 2. Application of our results on CRT based fixed patterns in combiner sequences are valid for any configuration of non linear combining function. However, point of concern for cryptanalysis is computaion of $\mathbf{S}_k$ in a typical scenerio of ciphertext only attack where limitataion of known keystream bits is always a driving factor for practability of the attack. For computations of DFT spectral

component, complete period of ciphertext is required which is practically not the case for cryptnalaysis attacks. Fast discrete fourier spectra attacks [8] provide an efficient methodology to compute particular spectral points when number of known bits are far less than the complete period of the stream. Our CRT based methodolgy can be utilized in conjunction with both the DFT finding algorithms proposed in [8] when number of known key stream bits are equal to linear span of the sequnece or even lesser than that. Detailed results on efficiency of this proposed methodology will be presented separately.

Remark 3. With regards to cryptanalysis attacks on combinatorial sequence generators, correlation attacks [13] and their faster variants [9] are conisdered to be the most efficient attacks [2]. Computational cost of our proposed methodology of DFT spectral points, even by employing fast discrete fourier spectra attacks, is more than correlation attacks. However, in a scenerio of correlation immune non linear boolean functions when coorelation attacks are not succesful, our proposed methodology of CRT based spectral computataions is still valid which will be addressed at a separate forum.

6 Conclusion

In this paper, new results on CRT based analysis of combinatorial sequences have been presented. We explored inherent peculiarities of the LFSR based combiner generators through novel patterns identified with the help of a CRT based approach. These findings were then extended to the product sequences and more particularly to the combinatorial generators. An effort was made to establish the mapping of different operations from time domain to frequency domain. Novel results on fixed shift patterns of LFSRs, their relationship to cyclic structures in finite fields and CRT based interpretation of these patterns have been exploited to establish direct relevance of final keystreams of combiner generators to individual LFSR sequences. Based on these CRT based fixed structures, new methodology of direct computating the spectral components of sequences in larger finite fields from constituent spectra of smaller fields is also presented. These new results on CRT based structural analysis of LFSR based combiners are demonstrated on small scale sequence generators with brief discussion on involved computational costs and practability of these techniques in cryptanalysis attacks.

References

1. RE Blahut. *Theory and practice of error control codes.* Addison-Wesley Publishing Company, USA, 1983.
2. Anne Canteaut. Stream cipher. *Encyclopedia of Cryptography and Security*, pages 1263–1265, 2011.
3. C Ding, D Pei, and A Salomaa. Chinese remainder theorem. applications in computing, coding, cryptography. 1996.

4. Solomon W Golomb and Guang Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, New York, USA, 2005.
5. Solomon Wolf Golomb, Lloyd R Welch, Richard M Goldstein, and Alfred W Hales. *Shift register sequences*, volume 78. Aegean Park Press Laguna Hills, CA, 1982.
6. Guang Gong. A closer look at selective dft attacks.
7. Guang Gong and Solomon W Golomb. Transform domain analysis of des. *Information Theory, IEEE Transactions on*, 45(6):2065–2073, 1999.
8. Guang Gong, Sondre Rønjom, Tor Helleseth, and Honggang Hu. Fast discrete fourier spectra attacks on stream ciphers. *Information Theory, IEEE Transactions on*, 57(8):5555–5565, 2011.
9. Willi Meier and Othmar Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, 1(3):159–176, 1989.
10. John M Pollard. The fast fourier transform in a finite field. *Mathematics of computation*, 25(114):365–374, 1971.
11. Irving S Reed and Trieu-Kien Truong. The use of finite fields to compute convolutions. *Information Theory, IEEE Transactions on*, 21(2):208–213, 1975.
12. Rainer A Rueppel. *Analysis and design of stream ciphers*. Springer-Verlag New York, Inc., 1986.
13. Thomas Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *Computers, IEEE Transactions on*, 100(1):81–85, 1985.